UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/777,602	02/13/2004	Hyun-Sook Lee	P56996	4949

7590 03/25/2008

Robert E. Bushnell
Suite 300
1522 K Street, N.W.
Washington, DC 20005

EXAMINER
HAILU, TESHOME

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
03/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/777,602	LEE, HYUN-SOOK	
	Examiner	Art Unit	
	TESHOME HAILU	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/17/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on December 17, 2007. Claims 1-12 have been amended.

2. Claims 1-12 are pending.

Response to Amendment

3. Applicant's arguments filed on December 17, 2007, with respect to the PTO-892, examiner filed the new PTO-892 form to include the prior art used in the first office action.

4. Applicant's arguments filed December 17, 2007, with respect to 35 USC(e) rejections of claims 1-12 have been fully considered but they are not persuasive.

5. Applicant argues that the combination of Dillon et al (US Pub. No. 2003/0172264) and Yang-huffman (US Pub. No. 2003/0115316) fails to teach "security method for operator access control of a network management system" and "confirming whether or not an IP address of a terminal used by the operator is a preset IP address" and "selectively accepting a request for the Simple Network Management Protocol (SNMP) packet if the raw is used as an egress policy". Examiner disagrees.

6. Examiner would point out that, Dillon teaches a secured communication over network (page 1, paragraph 2, the present invention relates to secure communication over a communication system). According to Dillon, the communication system is a network communication system such as an Internet.

7. Examiner would also point out that, Dillon teaches the claim limitation "confirming whether or not an IP address of a terminal used by the operator is a *preset* IP address" as (page 14, paragraph 145, the IP address of a TCP connection matches one or more of the IP address masks). Further Dillon disclosed

(page 10, paragraph 106, default rule can also be set which defines the action to be taken for IP packets which do not match any of the defined rules). Examiner interprets the word "preset" as a stored reference or rule.

8. Examiner would further point out that, Dillon teaches the claim limitation "selectively accepting a request for the Simple Network Management Protocol (SNMP) packet if the raw is used as an egress policy" as (page 10, paragraph 106, a rule can be defined to assign a priority for SNMP data received from a specific host). Examiner interprets the word "Selectively" as a rule (priority) to receive SNMP request. Examiner point out that the art on record teaches the claimed limitations and therefore, the rejection is respectfully maintained.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1, 6, 7 and 12 are rejected under 35 U.S.C. 102(e) as being anticipated by Dillon et al (Dillon), US Pub. No. 2003/0172264.

As per claim 1 Dillon discloses:

A security method for operator access control of a network management system, the method comprising: (page 2, paragraph 11, the method also includes filtering the plurality of packets, according to a security policy, to establish a connection for accelerating the filtered packets over a network)

Performing an Internet Protocol (IP) filtering to determine whether or not an inputted Internet Protocol address of an external operator is a preset Internet Protocol address using one of either a Transmission Control Protocol/Internet protocol (TCP/IP) or a User Datagram Protocol/Internet protocol (UDP/IP); (page 4, paragraph 46, this arrangement also permits the firewall 119 to have access to the data after the packet has been restored back to native TCP so that the firewall 119 can properly provide access control checking on the restored TCP connections and packets. Specifically, the firewall 119 controls the types of packets entering and leaving the PEP peer 101, using a number of methods, including packet filtering, proxy service, and stateful inspection, for example. The firewall 119 can apply various filters, which can be based on IP address).

Connecting the external operator to a communication system by either inputting an Identifier/Password or by setting communities upon a determination that the Internet Protocol address of the external operator is a preset Internet Protocol address. (Page 14, paragraph 145, as noted, the mapping of TCP connections to a PEP peer can be performed by a routing table (shown as "R"). In this example, the terminal 305 maintains the routing table, which identifies the PEP peer's IP address and contains one or more IP address masks in such a way that a destination IP address of a TCP connection matches one or more of the IP address masks).

Claim 7 is rejected under the same reason set forth in rejection of claim 1:

As per claim 6 Dillon discloses:

The security method according to claim 1, where the external operator comprises one of a telnet terminal or an Element Management System (EMS) server. (Page 14, paragraph 146, in one scenario, the host 301 seeks to communicate with the server 313 (e.g., web server) within the Internet).

Claim 12 is rejected under the same reason set forth in rejection of claim 6:

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 2-5 and 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dillon, US Pub. No. 2003/0172264, and further in view of Yang-Huffman, US Pub. No. 2003/0115316.

As per claim 2 Dillon discloses:

The security method according to claim 1, wherein performing an Internet Protocol (IP) filtering comprises: selecting whether to discard or accept a Simple Network Management Protocol (SNMP) packet to be inputted or outputted; (page 10, paragraph 110, as with the prioritization criteria (rules) the AND and OR combination operators can be used to link criteria together. For example, using the AND combination operator, a rule can be defined to select a path for SNMP data received from a specific host).

Selectively accepting a request for the Simple Network Management Protocol (SNMP) packet if the row is used as an egress policy, while not outputting a response packet; (page 10, paragraph 110, as with the prioritization criteria (rules) the AND/OR combination operators can be used to link criteria together. For example, using the AND combination operator, a rule can be defined to select a path for SNMP data received from a specific host) and (page 12, paragraph 126, egress prioritization is also applied before forwarding packets to the access network 307).

Selectively outputting the response packet for the Simple Network Management Protocol (SNMP) packet if the row is used as an ingress policy, while not allowing accepting the request for the Simple Network Management Protocol (SNMP) packet. (Page 10, paragraph 110, as with the prioritization criteria (rules) the AND/OR combination operators can be used to link criteria together. For

example, using the AND combination operator, a rule can be defined to select a path for SNMP data received from a specific host) and (page 12, paragraph 126, on the ingress side, prioritization is used to control access to buffer space and other resources in the PEP peer 107, generally and with respect to TCP spoofing).

Creating a row after setting a filtering range for objects that are implemented by a Management Information Base (MIB); (page 4, paragraph 46, the firewall 119 controls the types of packets entering and leaving the PEP peer 101, using a number of methods, including packet filtering, proxy service, and stateful inspection, for example. The firewall 119 can apply various filters, which can be based on IP address).

Dillon dose not explicitly discloses, Management Information Base (MIB). On the other hand, the same field of endeavor, Yang-Huffman teaches this limitation as, (page 1, paragraph 7, an SNMP GetNext operation is generally a command to retrieve information regarding a row in a MIB table which immediately succeeds a row identified by a particular OID). Where “retrieve information regarding a row in a MIB table” inherently indicate the row is created.

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Dillon and include the Management Information Base (MIB) using the teaching of Yang-Huffman. The modification would be obvious because one of ordinary skill in the art would be motivated to add a row that are implemented by a MIB to the system for having a better way of scanning a table to finding the value of an object. (Page1, Paragraph 8)

Claim 8 is rejected under the same reason set forth in rejection of claim 2:

As per claim 3, Dillon discloses

The security method according to claim 2, wherein creating a row after setting a filtering range for objects that are implemented by a Management Information Base (MIB) comprises: determining a PolicyId (PId) as to whether or not to adopt a certain packet processing method; (page 2, paragraph 11,

the method also includes filtering the plurality of packets, according to a security policy, to establish a connection for accelerating the filtered packets over a network).

Finding a row in a Filter Policy table, the row having a relevant value based on the determined PolicyId value; reading a pointer value of the row found in the FilterPolicy table; and finding a relevant row in a FilterIp table using the previously read pointer value as an index number, and then determining whether or not operator access is permitted based on conditions for an Internet Protocol (IP) address and a port number set in the relevant row to process a packet. (Abstract, line 1-5, an approach for providing integrated firewall and network acceleration functions is disclosed. An integrated firewall and network accelerator filters packets received from a host, according to a security policy, to establish a connection for accelerating the filtered packets over a network) and (page 4, paragraph 46, specifically, the firewall 119 controls the types of packets entering and leaving the PEP peer 101, using a number of methods, including packet filtering, proxy service, and stateful inspection, for example. The firewall 119 can apply various filters, which can be based on IP address, domain name, communication protocol, and port, for example).

Claim 9 is rejected under the same reason set forth in rejection of claim 3:

As per claim 4, Dillon discloses:

The security method according to claim 3, wherein the FilterIp table, in which items of the conditions for determining whether or not the operator access is permitted are recorded, comprises: an index number field using a pointer value corresponding to the policyId as an index, an Internet Protocol (IP) address field, an Internet Protocol (IP) address mask field, a port number field, a protocol field, a control field, and a row status field. (Page 4, paragraph 46, firewall 119 can properly provide access control checking on the restored TCP connections and packets. Specifically, the firewall 119 controls the types of packets entering and leaving the PEP peer 101, using a number of methods, including packet filtering, proxy service, and stateful inspection, for example. The firewall 119 can apply various filters, which can be based on IP address, domain name, communication protocol, and port, for example).

Further Dillon disclosed (page 14, paragraph 145, the terminal 305 maintains the routing table, which identifies the PEP peer's IP address and contains one or more IP address masks in such a way that a destination IP address of a TCP connection matches one or more of the IP address masks).

Claim 10 is rejected under the same reason set forth in rejection of claim 4:

As per claim 5 Dillon discloses:

A syntax of each of the Internet Protocol (IP) address field and the Internet Protocol (IP) address mask field is of an Internet Protocol (IP) address type. (Page 4, paragraph 46, the firewall 119 can apply various filters, which can be based on IP address domain name, communication protocol, and port).

The security method according to claim 4, wherein a syntax of each of the index number field, the port number field, the protocol field, the control field and the row status field is of an integer type (page 4, paragraph 46, firewall 119 can properly provide access control checking on the restored TCP connections and packets. Specifically, the firewall 119 controls the types of packets entering and leaving the PEP peer 101, using a number of methods, including packet filtering, proxy service, and stateful inspection, for example. The firewall 119 can apply various filters, which can be based on IP address, domain name, communication protocol, and port, for example"). Further Dillon disclosed (page 14, paragraph 145, "the terminal 305 maintains the routing table, which identifies the PEP peer's IP address and contains one or more IP address masks in such a way that a destination IP address of a TCP connection matches one or more of the IP address masks).

Dillon dose not explicitly discloses about integer type. On the other hand, the same field of endeavor, Yang-Huffman teaches this limitation as (page 1, paragraph 5, each object is generally associated with a unique identifier and generally consists of a sequence of integers).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made to modify the teaching of Dillon and include integers using the teaching of

Yang-Huffman. The modification would be obvious because one ordinary skill in the art would be motivated to add integers to the system for having a better way of identifying system.

Claim 11 is rejected under the same reason set forth in rejection of claim 5:

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

March 4, 2008

/Matthew Heneghan/
Primary Examiner, Art Unit 2139

.